

Symmetric Device-Independent Quantum Key Distribution Against General Attack

Yong-gang Tan*

*Physics and Information Engineering Department, Luoyang Normal College,
Luoyang 471022, Henan, People's Republic of China*

Abstract

A symmetric device-independent quantum key distribution (DIQKD) protocol is proposed in this paper, with Holevo limit and subadditivity of von Neumann entropy, one can bound Eve's ability with collective attack. Together with symmetry of this protocol, the state Eve prepared for Alice and Bob, and at the same time, her eavesdropping on Alice's and Bob's measurements can be definitely inferred at the assumption that Eve aims at maximizing her information gain. The optimal state under this circumstance can be solely bounded with Alice and Bob's statistical results on the quantity of Clauser-Horne-Shimony-Holt (CHSH) polynomial S , that is, our symmetric DIQKD has the same secure basis as that of Ekert91 protocol.

Keywords: device-independent, quantum key distribution, CHSH inequality, collective attack

PACS numbers: 03.67.Dd

*Electronic address: yonggang.tan@gmail.com

I. INTRODUCTION

Quantum key distribution (QKD) is an art of generating physically secure key between remote partners, the information sender Alice, and the receiver Bob [1–3], even if in the presence of a powerful eavesdropper, namely Eve, whose capability is only limited by quantum mechanics. On one hand, the security proof of QKD has been obtained with nearly perfect apparatus [4, 5]. On the other hand, there are different loopholes in current QKD experiments that may injure the security of the final key bits [6–12]. Even with the perfect experimental apparatus [4, 5], there are also some self-evident assumptions that guarantee the security of final key bits. For instance, we have to assume that Alice and Bob have the freedom to choose the bases for their preparations and measurements. Their classical results which is unwanted to be leaked out should be completely secret. At the same time, Alice and Bob should entirely control their apparatus to generate the raw keys. Or else, the final key bits cannot be secure.

As for commercial application, the apparatuses of Alice and Bob will be black boxes that may be provided by their potential rivals. It is interesting how Alice and Bob can determine the security of their final key bits extracted from these black boxes? Recently, the device-independent QKD (DIQKD) [13–15] has been suggested to ask for the answer. It was assumed in this protocol that Alice and Bob have no knowledge about their measurement devices. The violation of CHSH inequality will impose restriction on Hilbert space dimension of their measurements to ensure the efficient quantum correlations between Alice and Bob [16, 17]. Secure key bits against collective attack for this protocol has been proven [14, 15]. Its final key generation rate depends on two parameters, the quantity of CHSH polynomial S and the quantum bit error rate (QBER) Q . These two parameters are decided by the state measured by the legitimate users' devices and the way of their measurements at the same time. As Alice and Bob have no idea about the state prepared by Eve, and their measurement devices can also be fabricated by their rivals, generalization from collective attack to general attack is still missed.

The way of state preparation in DIQKD is the same as those of Ekert91 protocol [2] and entanglement-based QKD protocol with sources in the middle [18, 19] where Eve's eavesdropping ability is bounded with collective attack as quantum De Finetti theorem can be applied after Alice and Bob having randomized the measurement sequences on their

states [20, 21]. In DIQKD, however, It is impossible for Alice and Bob to make sure that their measurements function exactly on the quantum systems as their expectations. In fact, Eve may devise Alice's and Bob's measurements differently in every run. In this paper, a symmetric DIQKD protocol is proposed. The symmetry of this protocol, together with the Holevo limit [22–24], will provide strong confinements on Eve's eavesdropping. We show Eve's information is maximized when all states distributed to Alice and Bob are identically prepared. Then the procedure of uniform their states is completed automatically, and Alice and Bob can estimate their parameters by randomizing the sequences of their classical results. Furthermore, Eve's optimal state when her illegal information is maximized can be solely bounded with Alice and Bob's parameter S . Then our symmetric DIQKD has the same secure basis as that of Ekert91 protocol.

II. A SYMMETRIC DIQKD PROTOCOL

Our DIQKD protocol is symmetric not only because Alice's and Bob's basis choices are symmetric, but also because the statistical results generated from all bases are the same. It works as follows. (1) N EPR pairs emit from the signal source set between Alice's and Bob's labs. One particle of the EPR pair is sent to Alice and the other one is sent to Bob. (2) Both Alice and Bob choose four expecting measurement bases as $\theta_1 = \sigma_x$, $\theta_2 = (\sigma_x + \sigma_z)/\sqrt{2}$, $\theta_3 = \sigma_z$, $\theta_4 = (-\sigma_x + \sigma_z)/\sqrt{2}$ (As is shown in Fig. 1). In each run, Alice will randomly measure the incoming particle in one of the four bases, and so does Bob. (3) After all EPR pairs having been distributed, Alice and Bob announce the bases they used in each run through their classical channels. (4) Alice and Bob randomize the sequences of their classical results. They keep partial measurement results on the same bases as secrecy that will be used to generate secure final key bits. Then they publish all the other measurement results to estimate the disturbances and correlations on their sifted key bits. They abort their communication if the parameter estimation fails to meet their predefined requirements. Or else, they carry out privacy amplification to generate their secure final key.

Without loss of generality, we assume Eve prepares all Alice's and Bob's systems and her auxiliary systems in a big state $\rho_{A_1 \dots A_N B_1 \dots B_N E}$. Noting Alice's measurement operations as A_1 , A_2 , A'_1 and A'_2 , Bob's measurement operations as B_1 , B_2 , B'_1 and B'_2 , the joint measurements of Alice's and Bob's devices can then be depicted as $A_{i1}^{u_1}(t_1) \otimes B_{j1}^{v_1}(t_1) \cdots A_{iN}^{u_N}(t_N) \otimes B_{jN}^{v_N}(t_N)$.

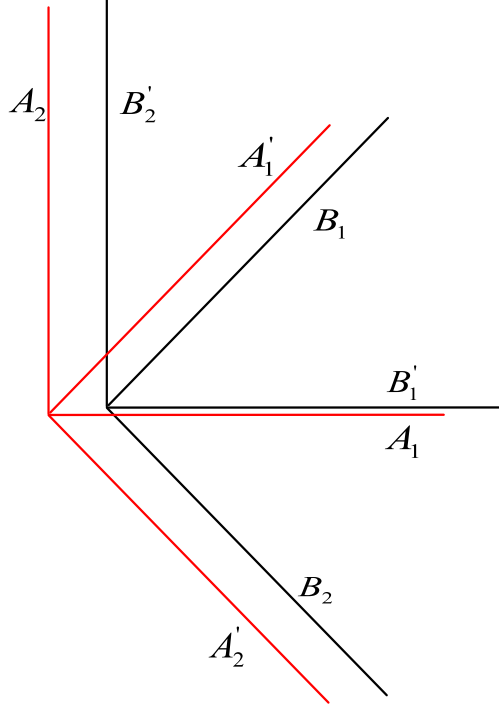


FIG. 1: Schematic for symmetric DIQKD. A_i s and A'_i s are Alice's possible basis choices. B_j s and B'_j s are Bob's basis choices.

Here t_1, \dots, t_N are sorted in time sequence as Eve may eavesdrop on Alice's and Bob's measurements differently in every run, $u_1, \dots, u_N, v_1, \dots, v_N$ correspond to the upper indexes, and i_1, \dots, i_N can be 1 or 2 randomly. As Eve's measurements will not affect the marginal distributions of Alice's and Bob's classical results, their results generated from $\rho_{A_1 \dots N B_1 \dots N E}$ can be depicted as $Tr[A_{i_1}^{u_1}(t_1) \otimes B_{j_1}^{v_1}(t_1) \dots A_{i_N}^{u_N}(t_N) \otimes B_{j_N}^{v_N}(t_N) Tr_E(\rho_{A_1 \dots N B_1 \dots N E})]$, where Tr_E is the trace on Eve's systems. According to DIQKD protocol, the result in the k th run is $Tr(A_{i_k}^{u_k}(t_k) \otimes B_{i_k}^{v_k}(t_k) (Tr_{A_1 \dots k-1 k+1 \dots N B_1 \dots k-1 k+1 \dots N E}(\rho_{A_1 \dots N B_1 \dots N E}))) = a^k b^k$, where a_k and b_k are the classical results obtained by Alice and Bob respectively. If they are binary, taking -1 and 1 for example, it is proven that $A_{i_k}^{u_k}(t_k)$ and $B_{i_k}^{v_k}(t_k)$ functioned on qubit states [14, 15, 25–27]. Furthermore, $A_{1_k}(t_k), A_{2_k}(t_k), B_{1_k}(t_k)$ and $B_{2_k}(t_k)$ can be set in the same plane $x - z$. Similarly, $A'_{1_k}(t_k), A'_{2_k}(t_k), B'_{1_k}(t_k)$ and $B'_{2_k}(t_k)$ can be set in another plane $x' - z'$ [14, 15].

Defining $Tr_{A_1 \dots k-1k+1 \dots N B_1 \dots k-1k+1 \dots N E}(\rho_{A_1 \dots N B_1 \dots N E}) \equiv \rho_{AB}^k$, the Hilbert space of Alice and Bob as H_{AB} , $\rho_{AB}^k \in H_{AB}$ and $\dim H_{AB} \leq 4$ should be satisfied. According to Holevo limit [22–24], Eve’s ability to distinguish the state shared by Alice and Bob is limited by $S(Tr_E(\rho_{A_1 \dots N B_1 \dots N E}))$, where $S(\rho) = -Tr(\rho \log_2(\rho))$ is the von Neumann entropy. If writing $\rho_{A_1 \dots N B_1 \dots N E}$ as $\rho_{A_1 \dots ss+1 \dots N B_1 \dots ss+1 \dots N E}$, $S(Tr_E(\rho_{A_1 \dots N B_1 \dots N E})) \leq S(Tr_{A_{s+1} \dots N B_{s+1} \dots N E}(\rho_{A_1 \dots N B_1 \dots N E})) + S(Tr_{A_1 \dots s B_1 \dots s E}(\rho_{A_1 \dots N B_1 \dots N E}))$ is required for the subadditivity of entropy. With the same procedure, one can have $S(Tr_E(\rho_{A_1 \dots N B_1 \dots N E})) \leq \sum_k S(Tr_{A_1 \dots k-1k+1 \dots N B_1 \dots k-1k+1 \dots N E}(\rho_{A_1 \dots N B_1 \dots N E}))$. The equality holds if and only if $Tr_E(\rho_{A_1 \dots N B_1 \dots N E})$ can be written as N product systems shared between Alice and Bob, that is, $Tr_E(\rho_{A_1 \dots N B_1 \dots N E}) = \otimes_{k=1}^N \rho_{AB}^k$.

Eve controls the transmission of quantum state, thus she can make ρ_{AB}^k optimal for her information gain. As $\dim H_{AB} \leq 4$, projective measurements can be launched on ρ_{AB}^k in a 4-dimensional Hilbert space H , with $H_{AB} \subseteq H$. Let $\sum_l P_{AB}^l = I$ be projective measurements in H , it is proven that $S(\sum_l P_{AB}^l \rho_{AB}^k P_{AB}^l) \geq S(\rho_{AB}^k)$. The equality holds if and only if $\rho_{AB}^k = \sum_l P_{AB}^l \rho_{AB}^k P_{AB}^l$ [24]. That is, $\sum_l P_{AB}^l \rho_{AB}^k P_{AB}^l$ can be diagonalized in bases $T = \{\tau_l\}$ with $\tau_l \tau_l^\dagger = P_{AB}^l$. Defining $\Lambda \equiv \sum_l P_{AB}^l \rho_{AB}^k P_{AB}^l = P^{-1} \rho_{AB}^k P$, then Λ is a diagonal matrix in H , and P is composed with the basis vectors $\{\tau^k\}$. Noticing Bell bases $B = \{\varsigma_l\}$ is also a set of bases in H , there should be a unitary operator U satisfying $T = UB$. Then one can have $\Lambda = B^{-1} U^{-1} \rho_{AB}^k U B$, which means ρ_{AB}^k can be diagonalized in Bell bases after it has been operated as $U^{-1} \rho_{AB}^k U$. It is apparently that this process will not alter the amount of entanglement on ρ_{AB}^k , and Eve’s information gain is only determined by the elements of Λ . That is, the assumption that the state ρ_{AB}^k can be diagonalized on Bell bases will not affect Eve’s information gain, and at the same time, it will not harm Eve’s ability to intervene Alice and Bob’s communication. Then it does not loss any generality to assume ρ_{AB}^k can be diagonalized on Bell bases so long as both Alice’s and Bob’s marginal distributions are symmetric [14, 15].

Suppose the state distributed by Eve in the k th run is $\sigma_{AB}^k \equiv (1 - p_k) \rho_{|\Phi^+\rangle} + p_{k1} \rho_{|\Phi^-\rangle} + p_{k2} \rho_{|\Psi^+\rangle} + p_{k3} \rho_{|\Psi^-\rangle}$, where $p_k = p_{k1} + p_{k2} + p_{k3}$, $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, $|\Phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$, $|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$, and $|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$. We now show that Eve’s information on Alice and Bob’s results is maximized when all σ_{AB}^k s are identically prepared.

(I) When there are only two types of quantum states equiprobably prepared on Alice and Bob’s N shared systems (This assumption does not loss any generality if these two states are prepared to be the same), they can be denoted as $\sigma_{AB}^{(\alpha)} = (1 - p^{(\alpha)}) \rho_{|\Phi^+\rangle} + p_1^{(\alpha)} \rho_{|\Phi^-\rangle} +$

$p_2^{(\alpha)}\rho_{|\Psi+\rangle} + p_3^{(\alpha)}\rho_{|\Psi-\rangle}$ and $\sigma_{AB}^{(\beta)} = (1 - p^{(\beta)})\rho_{|\Phi+\rangle} + p_1^{(\beta)}\rho_{|\Phi-\rangle} + p_2^{(\beta)}\rho_{|\Psi+\rangle} + p_3^{(\beta)}\rho_{|\Psi-\rangle}$. Then Eve's information gain on these states should be represented as $\frac{N}{2}S(\sigma_{AB}^{(\alpha)}) + \frac{N}{2}S(\sigma_{AB}^{(\beta)})$. If the statistical state on the N entangled systems measured by Alice and Bob is $\sigma_{AB} = (1 - p)\rho_{|\Phi+\rangle} + p_1\rho_{|\Phi-\rangle} + p_2\rho_{|\Psi+\rangle} + p_3\rho_{|\Psi-\rangle}$, we have $p_1^{(\alpha)} = p_1^{(\beta)} = p_1$, $p_2^{(\alpha)} = p_2^{(\beta)} = p_2$, and $p_3^{(\alpha)} = p_3^{(\beta)} = p_3$ when Eve's information gain is optimal.

(II) When there are m types of density matrixes equiprobably prepared by Eve, we assume Eve's illegal information is maximal only when all of them are identically prepared on the N entangled systems between Alice and Bob. That is, $S(\sigma_{AB}^{(\alpha)}) + S(\sigma_{AB}^{(\beta)}) + \dots + S(\sigma_{AB}^{(m)}) \leq mS(\sigma_{AB})$ is satisfied with the equality holds if and only if $\sigma_{AB}^{(\alpha)} = \sigma_{AB}^{(\beta)} = \dots = \sigma_{AB}^{(m)} = \sigma_{AB}$. Here σ_{AB} is the statistical expression on the N shared systems of Alice and Bob.

(III) When there are $m + 1$ types of states measured by Alice and Bob equiprobably, Eve's information gain on them can be written as $S_E = \frac{N}{m+1}[S(\sigma_{AB}^{(\alpha)}) + S(\sigma_{AB}^{(\beta)}) + \dots + S(\sigma_{AB}^{(m)}) + S(\sigma_{AB}^{(m+1)})]$. If the statistical expression for the first m types of states on the $\frac{m}{m+1}N$ systems is $\sigma_{AB}^{(\Omega)} = (1 - p^{(\Omega)})\rho_{|\Phi+\rangle} + p_1^{(\Omega)}\rho_{|\Phi-\rangle} + p_2^{(\Omega)}\rho_{|\Psi+\rangle} + p_3^{(\Omega)}\rho_{|\Psi-\rangle}$, S_E can be bounded as $\frac{N}{m+1}[mS(\sigma_{AB}^{(\Omega)}) + S(\sigma_{AB}^{(m+1)})]$ according to step (II). With simple calculation, one can obtain its maximum value when $\sigma_{AB}^{(\Omega)} = \sigma_{AB}^{(m+1)} = \sigma_{AB}$, with σ_{AB} being the statistical representation of all N shared systems between Alice and Bob. In conclusion, Eve should prepare the state on the N systems identically if she want to maximize her illegal information from Alice and Bob's communication. Then there is no need to randomize the measurement sequences to make their states uniformly distributed. Quantum De Finetti theorem can be applied in DIQKD protocol and Eve's information can be bounded with collective attack [20, 21].

Alice and Bob may not infer Eve's single intervention on their measurements in the k th run because of quantum randomness. As their states are identically prepared, however, they can deduce the equivalent operations averaged from all results. Denoting the equivalent operations in $x - z$ plane as A_1, A_2, B_1 and B_2 , their directions are assumed to be $\theta_1, \theta_2, \varphi_1$ and φ_2 respectively. Similarly, denoting the equivalent operations in $x' - z'$ plane as A'_1, A'_2, B'_1 and B'_2 , the corresponding directions for them are $\theta'_1, \theta'_2, \varphi'_1$ and φ'_2 . The CHSH polynomial can be calculated as $S = \sum_{i,j} \text{sign}(3.5 - i - j)\text{Tr}(A_i B_j \sigma_{AB})$, and $S' = \sum_{i,j} \text{sign}(3.5 - i - j)\text{Tr}(A'_i B'_j \sigma_{AB})$, with $i, j = 1, \text{ or } 2$, and $\text{sign}(x)$ getting the sign of x . Our symmetric DIQKD protocol requires $S = S'$, moreover, it requires that all $\text{sign}(3.5 - i - j)\text{Tr}(A_i B_j \sigma_{AB})$ s and $\text{sign}(3.5 - i - j)\text{Tr}(A'_i B'_j \sigma_{AB})$ s have the same value $\frac{S}{4}$. Then one can obtain $p_1 = p_2$, and $\theta_2 - \theta_1 = \frac{\pi}{2}$, $\varphi_2 - \varphi_1 = -\frac{\pi}{2}$, $\theta_2 - \varphi_1 = \frac{\pi}{4}$ and $\theta_1 - \varphi_2 = \frac{\pi}{4}$, or

$\theta_2 - \theta_1 = -\frac{\pi}{2}$, $\varphi_2 - \varphi_1 = \frac{\pi}{2}$, $\theta_2 - \varphi_1 = -\frac{\pi}{4}$ and $\theta_1 - \varphi_2 = -\frac{\pi}{4}$. With the same procedure, we can have the relationships among θ'_1 , θ'_2 , φ'_1 and φ'_2 . It is interesting to find that measurements satisfying the above relationships can be proven to maximize the value of S . For Alice and Bob, bigger S means less disturbances, then Eve should have the measurements of Alice and Bob in every run obeys the above relationships in order to conceal her existence.

Two important things may be reconsidered: what is the relationship between plane $x - z$ and $x' - z'$ and whether should Eve prepares the states for A_1 , A_2 , B_1 , B_2 and A'_1 , A'_2 , B'_1 , B'_2 with different systems? It is interesting to notice that both questions deal with the relationship between measurements and information. And they can be answered at the same time. If plane $x - z$ does not coincide with plane $x' - z'$, they belong to different Hilbert spaces. When Eve prepares the states on the same systems, generalized measurements are carried out inevitably when Eve distributes them in two different Hilbert spaces. This process will decrease Eve's information gain on the state [24]. However, when Eve prepares the states on plane $x - z$ and $x' - z'$ with different systems, monogamy of entanglement means that Alice's and Bob's results extracted on the same bases should be totally uncorrelated [28–30]. This will increase QBER on the key, that is, she will risk to be detected on line without gaining more information. Then for the sake of Eve's optimal information gain, and concealing her existence at the same time, the Hilbert space of $x - z$ coincides with that of $x' - z'$, and the states for them are prepared on the same systems correspondingly.

When $p_1 = p_2$, one can have the relationship $p_1 + p_3 = \frac{1}{2} - \frac{S}{4\sqrt{2}}$. If the measurement directions between Alice and Bob are well aligned, the QBER can be calculated as $p_1 + p_3$. Or else, it should be written as $Q = \frac{1 - (1 - p - p_3) \cos \vartheta}{2}$, where ϑ is the included angle between these measurement directions. This value is greater than that of the former. Then Alice's measurement bases should keep alignment with those of Bob, one can obtain $S = 2\sqrt{2}[1 - 2Q]$, which is the same as that in [14, 15]. In practical implementation of DIQKD, Alice and Bob can not obtain the value of p . Defining $q \equiv p + p_3$, we have $q = 1 - \frac{S}{2\sqrt{2}} = 2Q$. But the exact value of p_1 and p_3 is still unknown. As Eve's information on σ_{AB} can be written as $S(\sigma_{AB}) = -(1 - q + p_3) \log_2(1 - q + p_3) - 2p_1 \log_2 p_1 - p_3 \log_2 p_3$, however, we have $p_3 = \frac{q^2}{4}$ and $p_1 = \frac{q}{2} - \frac{q^2}{4}$ when $S(\rho_{AB})$ is maximal. That is, the optimal state for Eve's eavesdropping is $\sigma_{AB}^{optimal} = (1 - q + \frac{q^2}{4})\rho_{|\Phi^+\rangle} + (\frac{q}{2} - \frac{q^2}{4})\rho_{|\Phi^-\rangle} + (\frac{q}{2} - \frac{q^2}{4})\rho_{|\Psi^+\rangle} + \frac{q^2}{4}\rho_{|\Psi^-\rangle}$. Different to the cases where Alice and Bob having full control of their measurement devices [31–33], color noise is optimal for Eve in the DIQKD protocol. This is because Alice and Bob can calculate the

value of p accurately in the former but they can only estimate the value of q in the latter.

Until now, we have proven Eve's optimal information to be $S(\sigma_{AB}^{optimal})$. If its corresponding quantity of CHSH polynomial is $S^{optimal}$, however, can Eve's optimal information be bounded as $S(\sigma_{AB}^{optimal})$ when Alice and Bob's statistical value of S is equal to $S^{optimal}$? If not so, there must be another $\sigma_{AB}^{optimal'}$ with which Eve can obtain more illegal information. That is, $S(\sigma_{AB}^{optimal'}) > S(\sigma_{AB}^{optimal})$ is satisfied. According to the discussion above, $\sigma_{AB}^{optimal'}$ should also be represented as $\sigma_{AB}^{optimal'} = (1 - q' + \frac{q'^2}{4})\rho_{|\Phi+\rangle} + (\frac{q'}{2} - \frac{q'^2}{4})\rho_{|\Phi-\rangle} + (\frac{q'}{2} - \frac{q'^2}{4})\rho_{|\Psi+\rangle} + \frac{q'^2}{4}\rho_{|\Psi-\rangle}$. Its corresponding S can be calculated to be less than $2\sqrt{2}(1 - q')$. As $S(\sigma_{AB}^{optimal'}) > S(\sigma_{AB}^{optimal})$, one can have $S^{optimal} \leq 2\sqrt{2}(1 - q') \leq 2\sqrt{2}(1 - q)$. For Alice and Bob, great S means less information can be obtained by Eve, which means $S^{optimal}$ can bound Eve's illegal information. Generally, if the value of CHSH polynomial is S , Eve's illegal information should be less than $E(S) = -\frac{1}{4}(1 + \frac{S}{2\sqrt{2}})\log_2 \frac{1}{4}(1 + \frac{S}{2\sqrt{2}}) - \frac{1}{4}(1 - \frac{S}{2\sqrt{2}})\log_2 \frac{1}{4}(1 - \frac{S}{2\sqrt{2}}) - (\frac{1}{2} - \frac{S^2}{16})\log_2(\frac{1}{4} - \frac{S^2}{32})$. Thus, DIQKD can be bounded with the quantity of CHSH polynomial, which means it has the same secure basis as that of Ekert91 protocol [2]. For collective attack, Alice and Bob's key generation can be represented as $r = 1 - H_2(Q) - \chi$, where $H_2(Q) = -Q\log_2 Q - (1 - Q)\log_2(1 - Q)$ is the Shannon entropy and χ is the Holevo limit [34, 35]. In our symmetric DIQKD, the lower bound of Alice and Bob's key generation rate can be estimated as $r \geq 1 - H_2(Q) - S(\sigma_{AB}^{optimal})$. If the relationship $S = 2\sqrt{2}(1 - 2Q)$ is satisfied, the key rate of our DIQKD can be calculated as

$$r \geq 1 - H_2(\frac{1}{2} - \frac{S}{4\sqrt{2}}) - E(S). \quad (1)$$

III. DISCUSSION AND CONCLUSION

In this paper, a symmetric DIQKD has been proposed, where Eve's ability of eavesdropping can be bounded with collective attack. That is, generalization on the security of DIQKD from collective attack to general attack can be realized. Its security can be estimated similarly as that of Ekert91 protocol, that is, determined by the quantity of CHSH polynomial S . However, we have only considered an ideal case where the loss in the quantum channel is not added in. In practical implementation of this protocol, there may be detecting loophole because of imperfectly detecting efficiency [32, 33]. Especially, faking state attack has been proposed to eavesdrop on DIQKD protocols with inefficient measurement devices [36]. To make DIQKD more practically with present devices, however, proposition

for experimental realization of this protocol has been given [37]. Besides its attractiveness of practical application, DIQKD is physically interesting as it provides us a way to understand the nonlocality of quantum principles, with which the legitimate users can set up secure communication without any knowledge about their quantum objects. The author thank helpful discussion from Q.-Y. Cai and X. Ma. This work is sponsored by the National Natural Science Foundation of China (Grant No 10905028) and HASTIT.

- [1] C. H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing*, Bangalore, India (IEEE, New York), PP. 175 (1984).
- [2] A. K. Ekert, *Phys. Rev. Lett.* **67**, 661 (1991).
- [3] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, *Rev. Mod. Phys.* **74**, 145 (2002).
- [4] H.-K. Lo and H. F. Chau, *Science* **283**, 2050C2056 (1999).
- [5] P. W. Shor and J. Preskill, *Phys. Rev. Lett.* **85**, 441 (2000).
- [6] B. Huttner, N. Imoto, N. Gisin and T. Mor, *Phys. Rev. A* **51**, 1863 (1995).
- [7] B. Qi, C.-H. F. Fung, H.-K. Lo and X. Ma, *Quant. Inf. Comp.* **7**, pp. 73-82 (2007).
- [8] Y. Zhao, C.-H. F. Fung, B. Qi, C. Chen and H.-K. Lo, *Phys. Rev. A* **78**, 042333 (2008).
- [9] C.-H. F. Fung, B. Qi, K. Tamaki and H.-K. Lo, *Phys. Rev. A* **75**, 032314 (2007).
- [10] F. Xu, B. Qi and H.-K. Lo, *New J. Phys.* **12**, 113026 (2010).
- [11] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar and V. Makarov, *Nature Photonics* **4**, pp. 686-689 (2010); Z. L. Yuan, J. F. Dynes and A. J. Shields, *Nature Photonics* **4**, pp. 800-801 (2010); L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar and V. Makarov, *Nature Photonics* **4**, 801 (2010).
- [12] I. Gerhardt, Q. Liu, A. Lamas-Linares, J. Skaar, C. Kurtsiefer and V. Makarov, *Nature Comm.* **2**, 349 (2011).
- [13] D. Mayers and A. C.-C. Yao, in *Proceedings of the 39th Annual Symposium on Foundations of Computer Science (FOCS98)*, (IEEE Computer Society, Washington, DC, 1998), p. 503.
- [14] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio and V. Scarani, *Phys. Rev. Lett.* **98**, 230501 (2007);
- [15] S. Pironio, A. Acín, N. Brunner, N. Gisin, S. Massar and V. Scarani, *New J. Phys.* **11**, 045021

- (2009).
- [16] J. Clauser *et. al.*, *Phys. Rev. Lett.* **23**, 880 (1969).
 - [17] J. S. Bell, *Physica* **1**, 195 (1965).
 - [18] X. Ma , C.-H. F. Fung , and H.-K. Lo, *Phys. Rev. A* **76** 012307, (2007).
 - [19] R. Renner, N. Gisin, B. Kraus, *Phys. Rev. A* **72**, 012332 (2005).
 - [20] R. Renner, Ph.D. thesis, ETH No. 16242, arXiv:quant-ph/ 0512258.
 - [21] R. Renner, *Nature Phys.* **3**, 645 (2007).
 - [22] A. S. Holevo, *Probl. Peredachi. Inf.*, **9**, 3 (1973).
 - [23] A. Cabello, *Phys. Rev. Lett.*, **85**, 5635 (2000).
 - [24] M. A. Nielsen, and I. L. Chuang, *Quantum computation and quantum information*. Cambridge University Press, (2000).
 - [25] B. S. Tsirelson . *Lett. Math. Phys.*, **4**, 93 (1980).
 - [26] B. Tsirelson, *Hadronic Journal Supplement*, **8**, 329 (1993).
 - [27] L. Masanes, *Phys. Rev. Lett.*, **97**, 050503 (2006).
 - [28] D. Bruß, *Phys. Rev. A*, **60**, 4344 (1999).
 - [29] V. Coffman, J. Kundu, and W. K. Wootters, *Phys. Rev. A*, **61** 052306 (2000).
 - [30] M. Koashi, and A. Winter, *Phys. Rev. A* **69**, 022309 (2004).
 - [31] P. H. Eberhard, *Phys. Rev. A*, **47**, R747 (1993).
 - [32] N. Brunner, N. Gisin, V. Scarani, and C. Simon, *Phys. Rev. Lett.*, **98**, 220403 (2007).
 - [33] A. Cabello and J.-A. Larsson, *Phys. Rev. Lett.* **98**, 220402 (2007).
 - [34] E. Biham and T. Mor, *Phys. Rev. Lett.*, **79**, 4034 (1997).
 - [35] E. Biham and T. Mor. *Phys. Rev. Lett.*, **78**, 2256 (1997).
 - [36] I. Gerhardt, Q. Liu, A. Lamas-Linares, J. Skaar, V. Scarani, V. Makarov, and C. Kurtsiefer, *Phys. Rev. Lett.*, **107**, 170404 (2011).
 - [37] N. Gisin, S. Pironio, and N. Sangouard, *Phys. Rev. Lett.*, **105**, 070501 (2010).

Appendix A: Bounding Eve’s information with Holevo limit

In DIQKD, Alice and Bob measure on the state ρ prepared by Eve. According to the Holevo limit, Eve’s illegal information on the results of Alice and Bob can be bounded with $S(\rho)$. If ρ is composed with many subsystems, that is, $\rho = \rho_{1,2,\dots,n}$. $S(\rho)$ can be proven to

satisfy the relationship

$$S(\rho) \leq \sum_{i=1}^n S(\rho_i), \quad (\text{A1})$$

where ρ_i is the state functions with Alice and Bob's measurements in the i th run. This conclusion can easily be proven with Klein's inequality $S(\rho) \leq -\text{Tr}(\rho \log_2 \sigma)$. Defining $\rho \equiv \rho_{1,2,\dots,n}$, $\sigma \equiv \otimes_{i=1}^n \rho_i$, and substituting them into the Klein's inequality, we have

$$\begin{aligned} S(\rho_{1,2,\dots,n}) &\leq -\text{Tr}(\rho_{1,2,\dots,n} \log_2 \otimes_{i=1}^n \rho_i) \\ &= -\text{Tr}(\rho_{1,2,\dots,n} (\log_2 \prod_{i=1}^n \rho_i)) \\ &= -\text{Tr}(\rho_{1,2,\dots,n} (\sum_{i=1}^n \log_2 \rho_i)) \\ &= \sum_{i=1}^n S(\rho_i). \end{aligned} \quad (\text{A2})$$

The equality holds if and only if the state can be written as product states of n systems.

Appendix B: Diagonalizing ρ_{AB} on Bell bases

Suppose P_i is a complete set of orthogonal projectors and ρ is a density operator. Then the entropy of the state $\sigma \equiv \sum_i P_i \rho P_i$ of the system after the measurement is at least as greater as the original entropy

$$S(\sigma) \geq S(\rho). \quad (\text{B1})$$

This results can be verified easily with Klein's inequality.

$$\begin{aligned} S(\rho) &\leq -\text{Tr}(\rho \log_2 \sigma) \\ &= -\text{Tr}(\sum_i P_i \rho \log_2 \sigma) \\ &= -\text{Tr}(\sum_i P_i P_i \rho \log_2 \sigma) \\ &= -\text{Tr}(\sum_i P_i \rho \log_2 \sigma P_i) \\ &= -\text{Tr}(\sum_i P_i \rho P_i \log_2 \sigma) \\ &= S(\sigma). \end{aligned} \quad (\text{B2})$$

If P_i s are the set of projective operators which can maximize Eve's information after it has functioned on state ρ . Writing P_i as $\tau_i \tau_i^\dagger$, then $T = \{\tau_i\}$ is the basis of the Hilbert space of ρ , and ρ is diagonal in basis $T = \{\tau_i\}$. Then σ is the diagonalized density matrix of ρ on basis $T = \{\tau_i\}$.

Now we will show ρ can be diagonalized in any other set of bases of the Hilbert space of ρ . If Q_i s are another set of projective operators in this Hilbert space, and $Q_i = \varsigma_i \varsigma_i^\dagger$,

$V = \{\varsigma_i\}$ s are also orthogonal bases of the Hilbert space of ρ . Similarly, we can define matrix Q constituting of bases $V = \{\varsigma_i\}$, then there exists a unitary matrix U , with which the relationship $P = UQ$ can be satisfied. We can rewrite density matrix σ as $\sigma = Q^{-1}U^{-1}\rho UQ$. That is, ρ can be diagonalized on basis $V = \{\varsigma_i\}$ after Eve operating it as $U^{-1}\rho U$. That is, if a quantum state can be diagonalized on one basis in the Hilbert space of ρ , it can be diagonalized on any other bases in this Hilbert space by just rotating the states with some unitary operation.

In DIQKD, Alice's and Bob's classical results are binary, it is proven that their measurements can extract qubit information from the states on the incoming particles. Then the state measured by Alice's and Bob's devices are confined in the Hilbert space H_{AB} , with $\dim H_{AB} \leq 4$. That is, Bell basis is a set of basis in this Hilbert space. Then if Eve can diagonalize state ρ with projective operators in the Hilbert space of H_{AB} , she can diagonalize it on Bell basis.

Appendix C: Alice and Bob's states should be identically prepared if Eve want her illegal information maximized

This conclusion can be proven with simple mathematical technique. Suppose there are m types states prepared for Alice and Bob.

(1) When $m = 1$, all states are identical.

(2) When $m = 2$, they are denoted as $\rho_{AB}^{(\alpha)} = (1-p^{(\alpha)})\rho_{|\Phi+\rangle} + p_1^{(\alpha)}\rho_{|\Phi-\rangle} + p_2^{(\alpha)}\rho_{|\Psi+\rangle} + p_3^{(\alpha)}\rho_{|\Psi-\rangle}$ and $\rho_{AB}^{(\beta)} = (1-p^{(\beta)})\rho_{|\Phi+\rangle} + p_1^{(\beta)}\rho_{|\Phi-\rangle} + p_2^{(\beta)}\rho_{|\Psi+\rangle} + p_3^{(\beta)}\rho_{|\Psi-\rangle}$. And their statistical representation of all systems can be written as $\rho_{AB} = (1-p)\rho_{|\Phi+\rangle} + p_1\rho_{|\Phi-\rangle} + p_2\rho_{|\Psi+\rangle} + p_3\rho_{|\Psi-\rangle}$. These two types of states are assumed to be prepared equiprobably, and this assumption does not loss any generality if these two types of states can be proven to be the same.

Then Eve's information gain on these states should be less than $\frac{N}{2}[S(\rho_{AB}^\alpha) + S(\rho_{AB}^\beta)]$, with N is the number of the total systems shared between Alice and Bob. One can then have

$$\begin{aligned} p_1^{(\alpha)} + p_1^{(\beta)} &= 2p_1, \\ p_2^{(\alpha)} + p_2^{(\beta)} &= 2p_2, \\ p_3^{(\alpha)} + p_3^{(\beta)} &= 2p_3, \end{aligned} \tag{C1}$$

and

$$\begin{aligned}
S_E &= \frac{N}{2}[S(\rho_{AB}^\alpha) + S(\rho_{AB}^\beta)] \\
&= -p_1^{(\alpha)} \log_2 p_1^{(\alpha)} - p_2^{(\alpha)} \log_2 p_2^{(\alpha)} - p_3^{(\alpha)} \log_2 p_3^{(\alpha)} \\
&\quad - (1 - p_1^{(\alpha)} - p_2^{(\alpha)} - p_3^{(\alpha)}) \log_2 ((1 - p_1^{(\alpha)} - p_2^{(\alpha)} - p_3^{(\alpha)})) \\
&\quad - p_1^{(\beta)} \log_2 p_1^{(\beta)} - p_2^{(\beta)} \log_2 p_2^{(\beta)} - p_3^{(\beta)} \log_2 p_3^{(\beta)} \\
&\quad - (1 - p_1^{(\beta)} - p_2^{(\beta)} - p_3^{(\beta)}) \log_2 ((1 - p_1^{(\beta)} - p_2^{(\beta)} - p_3^{(\beta)}))
\end{aligned} \tag{C2}$$

Substituting the relation in Eq. (7) into Eq. (8), we have $S_E = S_E(p_1^{(\alpha)}, p_2^{(\alpha)}, p_3^{(\alpha)})$. Varying $p_1^{(\alpha)}$, $p_2^{(\alpha)}$, and $p_3^{(\alpha)}$ to make S_E maximal, we can then have $p_1^{(\alpha)} = p_1^{(\beta)} = p_1$, $p_2^{(\alpha)} = p_2^{(\beta)} = p_2$, and $p_3^{(\alpha)} = p_3^{(\beta)} = p_3$.

(3) Suppose all types of states are identically prepared on the N systems for Eve's maximal information gain when $m = M \geq 3$. That is, Eve should make her eavesdropping optimal if M types of states are prepared on the N systems shared between Alice and Bob, $\rho_{AB}^{(\alpha)} = \rho_{AB}^{(\beta)} = \dots = \rho_{AB}^{(M)} = \rho_{AB}$ are required, with ρ_{AB} is the statistical state on the N systems. That is, $S_E = \frac{N}{M}[S(\rho_{AB}^{(\alpha)}) + S(\rho_{AB}^{(\beta)}) + \dots + S(\rho_{AB}^{(M)})] = NS(\rho_{AB})$ calculates the optimal information obtain by Eve.

(4) When $m = M + 1$, we still assume all states are prepared equiprobably. Then $S_E = \frac{N}{M+1}[S(\rho_{AB}^{(\alpha)}) + S(\rho_{AB}^{(\beta)}) + \dots + S(\rho_{AB}^{(M)}) + S(\rho^{(M+1)})]$. Suppose the statistical representation for the first M types of density matrix is ρ_{AB}^Ω ,

$$\begin{aligned}
S_E &= \frac{N}{M+1}[S(\rho_{AB}^{(\alpha)}) + S(\rho_{AB}^{(\beta)}) + \dots + S(\rho_{AB}^{(M)}) + S(\rho^{(M+1)})] \\
&= \frac{M}{M+1} \frac{N}{M}[S(\rho_{AB}^{(\alpha)}) + S(\rho_{AB}^{(\beta)}) + \dots + S(\rho_{AB}^{(M)})] + \frac{N}{M+1} S(\rho^{(M+1)}) \\
&\leq \frac{NM}{M+1} S(\rho_{AB}^\Omega) + \frac{N}{M+1} S(\rho^{(M+1)}).
\end{aligned} \tag{C3}$$

Denoting $\rho_{AB}^\Omega = (1 - p^{(\Omega)})\rho_{|\Phi+\rangle} + p_1^{(\Omega)}\rho_{|\Phi-\rangle} + p_2^{(\Omega)}\rho_{|\Psi+\rangle} + p_3^{(\Omega)}\rho_{|\Psi-\rangle}$, and $\rho^{(M+1)AB} = (1 - p^{(M+1)})\rho_{|\Phi+\rangle} + p_1^{(M+1)}\rho_{|\Phi-\rangle} + p_2^{(M+1)}\rho_{|\Psi+\rangle} + p_3^{(M+1)}\rho_{|\Psi-\rangle}$, with similar procedure as that in step (2), we have $p_1^{(\Omega)} = p_1^{(M+1)} = p_1$, $p_2^{(\Omega)} = p_2^{(M+1)} = p_2$, and $p_3^{(\Omega)} = p_3^{(M+1)} = p_3$. That is, the $M+1$ types of states are also required to be identical for Eve's optimal eavesdropping. Then all states on the N systems shared between Alice and Bob should be identically prepared if Eve want to maximize her illegal information.

Appendix D: Bounding Eve's eavesdropping on Alice's and Bob's measurements

Denoting the equivalent operations in $x-z$ plane as A_1 , A_2 , B_1 and B_2 , their directions are assumed to be θ_1 , θ_2 , φ_1 and φ_2 respectively. Similarly, denoting the equivalent operations

in $x' - z'$ plane as A'_1 , A'_2 , B'_1 and B'_2 , the corresponding directions for them are θ'_1 , θ'_2 , φ'_1 and φ'_2 . The state Eve prepares on Alice and Bob's shared systems is $\rho_{AB} = (1-p)\rho_{|\Phi^+\rangle} + p_1\rho_{|\Phi^-\rangle} + p_2\rho_{|\Psi^+\rangle} + p_3\rho_{|\Psi^-\rangle}$. Then $S = (1-p-p_3)[\cos(\theta_1 - \varphi_1) + \cos(\theta_1 - \varphi_2) + \cos(\theta_2 - \varphi_1) - \cos(\theta_2 - \varphi_2)] - (p_1 - p_2)[\cos(\theta_1 + \varphi_1) + \cos(\theta_1 + \varphi_2) + \cos(\theta_2 + \varphi_1) - \cos(\theta_2 + \varphi_2)]$ can be obtained. Furthermore, the correlation results on neighbour bases can be depicted as $S_{A_1B_1} = (1-p-p_3)\cos(\theta_1 - \varphi_1) - (p_1 - p_2)\cos(\theta_1 + \varphi_1)$, $S_{A_1B_2} = (1-p-p_3)\cos(\theta_1 - \varphi_2) - (p_1 - p_2)\cos(\theta_1 + \varphi_2)$, $S_{A_2B_1} = (1-p-p_3)\cos(\theta_2 - \varphi_1) - (p_1 - p_2)\cos(\theta_2 + \varphi_1)$, and $-S_{A_2B_2} = (1-p-p_3)\cos(\theta_2 - \varphi_2) - (p_1 - p_2)\cos(\theta_2 + \varphi_2)$ respectively. The symmetry of our DIQKD requires $S_{A_1B_1} = S_{A_1B_2} = S_{A_2B_1} = -S_{A_2B_2} = \frac{S}{4}$, then we have

$$\begin{aligned}
& (1-p-p_3)\cos(\theta_1 - \varphi_1) - (p_1 - p_2)\cos(\theta_1 + \varphi_1), \\
& = (1-p-p_3)\cos(\theta_1 - \varphi_2) - (p_1 - p_2)\cos(\theta_1 + \varphi_2), \\
& = (1-p-p_3)\cos(\theta_2 - \varphi_1) - (p_1 - p_2)\cos(\theta_2 + \varphi_1), \\
& = -(1-p-p_3)\cos(\theta_2 - \varphi_2) + (p_1 - p_2)\cos(\theta_2 + \varphi_2).
\end{aligned} \tag{D1}$$

Based on these relationships, we can obtain

$$\begin{aligned}
(1-p-p_3)\sin\left(\frac{2\theta_1-\varphi_1-\varphi_2}{2}\right)\sin\left(\frac{\varphi_1-\varphi_2}{2}\right) &= -(p_1-p_2)\sin\left(\frac{2\theta_1+\varphi_1+\varphi_2}{2}\right)\sin\left(\frac{\varphi_1-\varphi_2}{2}\right), \\
(1-p-p_3)\sin\left(\frac{2\varphi_1-\theta_1-\theta_2}{2}\right)\sin\left(\frac{\theta_1-\theta_2}{2}\right) &= -(p_1-p_2)\sin\left(\frac{2\varphi_1+\theta_1+\theta_2}{2}\right)\sin\left(\frac{\theta_1-\theta_2}{2}\right), \\
(1-p-p_3)\cos\left(\frac{2\theta_2-\varphi_1-\varphi_2}{2}\right)\cos\left(\frac{\varphi_1-\varphi_2}{2}\right) &= (p_1-p_2)\cos\left(\frac{2\theta_2+\varphi_1+\varphi_2}{2}\right)\cos\left(\frac{\varphi_1-\varphi_2}{2}\right), \\
(1-p-p_3)\cos\left(\frac{2\varphi_2-\theta_1-\theta_2}{2}\right)\cos\left(\frac{\theta_1-\theta_2}{2}\right) &= (p_1-p_2)\cos\left(\frac{2\varphi_2+\theta_1+\theta_2}{2}\right)\cos\left(\frac{\theta_1-\theta_2}{2}\right).
\end{aligned} \tag{D2}$$

As S should violate its classical bound 2, it is reasonable to assume that the value $p_1+p_2+p_3$ is small. Then $(1-p-p_3)$ is comparable with 1. If $\cos(\frac{\varphi_1-\varphi_2}{2}) = 0$, $\cos(\frac{\theta_1-\theta_2}{2}) = 0$, $\sin(\frac{\varphi_1-\varphi_2}{2}) = 0$, or $\sin(\frac{\theta_1-\theta_2}{2}) = 0$, one can obtain $S \leq 2$, which is not expected in DIQKD.

Then Eq. (D2) can be simplified as

$$\begin{aligned}
(1-p-p_3)\sin\left(\frac{2\theta_1-\varphi_1-\varphi_2}{2}\right) &= -(p_1-p_2)\sin\left(\frac{2\theta_1+\varphi_1+\varphi_2}{2}\right), \\
(1-p-p_3)\sin\left(\frac{2\varphi_1-\theta_1-\theta_2}{2}\right) &= -(p_1-p_2)\sin\left(\frac{2\varphi_1+\theta_1+\theta_2}{2}\right), \\
(1-p-p_3)\cos\left(\frac{2\theta_2-\varphi_1-\varphi_2}{2}\right) &= (p_1-p_2)\cos\left(\frac{2\theta_2+\varphi_1+\varphi_2}{2}\right), \\
(1-p-p_3)\cos\left(\frac{2\varphi_2-\theta_1-\theta_2}{2}\right) &= (p_1-p_2)\cos\left(\frac{2\varphi_2+\theta_1+\theta_2}{2}\right).
\end{aligned} \tag{D3}$$

If both sides of Eq. (D3) are not equal to 0, one can obtain

$$\begin{aligned}
\sin(\theta_1 + \theta_2) + \sin(\theta_1 - \theta_2)\cos(\varphi_1 + \varphi_2) &= 0, \\
\sin(\varphi_1 + \varphi_2) + \sin(\varphi_1 - \varphi_2)\cos(\theta_1 + \theta_2) &= 0.
\end{aligned} \tag{D4}$$

We can find the maximal value conditioned on the relationships in (D4), we find $S \leq 2$ in this condition. By further calculation, we can find that $\sin(\frac{2\theta_1+\varphi_1+\varphi_2}{2})$, $\sin(\frac{2\varphi_1+\theta_1+\theta_2}{2})$, $\cos(\frac{2\theta_2+\varphi_1+\varphi_2}{2})$, and $\cos(\frac{2\varphi_2+\theta_1+\theta_2}{2})$ can not be equal to 0 at the assumption of $S > 2$. Then we have $p_1 = p_2$ should be satisfied. And at the same time, we have $\theta_2 - \theta_1 = \frac{\pi}{2}$, $\varphi_2 - \varphi_1 = -\frac{\pi}{2}$, $\theta_2 - \varphi_1 = \frac{\pi}{4}$ and $\theta_1 - \varphi_2 = \frac{\pi}{4}$, or $\theta_2 - \theta_1 = -\frac{\pi}{2}$, $\varphi_2 - \varphi_1 = \frac{\pi}{2}$, $\theta_2 - \varphi_1 = -\frac{\pi}{4}$ and $\theta_1 - \varphi_2 = -\frac{\pi}{4}$.